UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**DOCKET NO. 16-CR-10305-NMG**
	)	
MARTIN GOTTESFELD	)	

DEFENDANT'S REPLY TO GOVERNMENT'S OPPOSITION TO MOTION TO SUPPRESS EVIDENCE

The government opposed Mr. Gottesfeld's Motion to Suppress Evidence on October 6, 2017. D.E. 84. Mr. Gottesfeld hereby replies to several discrete arguments made by the government. He does not repeat facts, information, or arguments set forth in either the Motion or Opposition.

Reasonable Expectation of Privacy in Defendant's Internet Information (Response to Govt. Opp. at 9-14)

Gottesfeld agrees with the governing test, *see Katz v. United States,* 389 U.S. 347 (1967), which the government lays out at page 9 of its Opposition (D.E. 84, "Govt. Opp."). The government first contends that Gottesfeld fails to show a subjective expectation of privacy in his internet information because he has not submitted an affidavit stating that he expected that his activities on the internet were private. Nor did the defendant in *Katz,* for that matter, need to submit an affidavit saying he thought his conversations in the phone booth were private. *See Katz*, 389 U.S. at 361 ("The critical fact in this case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted" (Harlan, J., concurring)). The question presented here is whether one has a reasonable expectation of privacy in information turned over to a third party for purposes of obtaining services. That question has been framed, through the third party doctrine, as one of law – not one of fact. *See, e.g., United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017) ("In light of the *Smith*

rule, no reasonable person could maintain a privacy interest in that sort of information"). Gottesfeld's Fourth Amendment argument is thus distinct from those suppression cases in which a search of a particular place indisputably took place but the defendant must establish that s/he had a subjective expectation of privacy *in that place* in order to have standing to object. *See, e.g., United States v. Bryant*, No. 07-CR-20043, 2008 WL 4724282, at *5 (C.D. Ill. Oct. 24, 2008) (discussing the matter as one of standing). That Gottesfeld expected his activities, undertaken through an encrypted server and from the privacy of his home, to be private seems to be a commonsense proposition. If the Court believes its determination hinges on an affidavit, Gottesfeld can easily provide one.

Second, the government argues that the *Smith* /third party rule is consistent with society's expectations. *See* Govt. Opp. at 11. It claims that Congress's expansion of the Pen/Trap Act, through the Patriot Act, "buttressed" the third party rule by adding internet communications to the Pen/Trap statute. Govt. Opp. at 11. However, the Patriot Act cannot override the Constitution. And the Constitution asks what contemporary society expects. *See United States v. Jones*, 565 U.S. 400, 417-18 (Sotomayor, J.); *see also Riley v. California*, 134 S. Ct. 2473, 2490 (2014). Contrary to the government's position, public opinion suggests that society today views electronic information as highly personal and is concerned about government surveillance. A bipartisan poll in 2015 found that "60 percent of Americans believe the Patriot Act should be reformed 'to limit government surveillance and protect Americans' privacy.'" Walker, L., "Poll: Majority of Americans Want the Patriot Act Reformed." *Newsweek* (May 18, 2015).[1] Indeed, "[m]ore than 80 percent of respondents [we]re 'concerned' that the government is 'collecting and storing Americans' personal information,' while 18 percent [we]re not." *Id.* Thus, Gottesfeld contends, Americans reasonably expect privacy in

[1] Available at: http://www.newsweek.com/poll-majority-americans-want-patriot-act-reformed-332991

the information they share with third parties, over the internet, for the purpose of obtaining services. *See Jones*, 565 U.S. at 417-18 (Sotomayor, J.).

Third, the government attempts to debunk the proposition that collecting information which may be constitutionally innocuous in granular form may nonetheless, at some level of aggregation, become constitutionally offensive. *See* Govt. Opp. at 12. In *Jones*, five members of the Court thought that even though a person makes his location public by travelling on public thoroughfares, he does not reasonably expect his whereabouts to be surveilled 24 hours per day for a month by the government. *See* Govt. Opp. at 12. It is true that the majority opinion in *Jones* rested its Fourth Amendment holding on a theory of physical trespass (the attachment of the physical GPS device to the car). *See id.* But the government ignores the explicit discussion by five members of the Court who agreed that an individual has a reasonable expectation of privacy in the "sum," or aggregation, of his movements, even though each of those movements is public. Justice Sotomayor joined the majority because the physical intrusion was a narrower basis for the decision, rendering "resolution of the difficult [*Katz*] questions … unnecessary." *Id.* at 418. However, the four-Justice concurrence written by Justice Alito would have held *solely* under the *Katz* framework that 28 days-worth of continuous data collection violated a reasonable expectation of privacy. *See id.* at 430 ("relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable …. [but] the line was surely crossed before the 4-week mark"). And Justice Sotomayor's view appears to be even more expansive: she warned that "even short-term monitoring …. will require particular attention" "in the digital age," and invited the Court to "reconsider the premise that an individual has no reasonable expectation of privacy in the information voluntarily disclosed to third parties." *Id.* at 415, 417.

Here, Gottesfeld's internet communications – his cyber-location – was monitored continuously, in real-time, 24 hours a day for 60 days. *See* PRTT Application ("PRTT App."), D.E.

2, at 5 (requesting access to the pen/trap information "continuously, 24 hours per day, so that the information will be furnished to the government during, or immediately after, the transmission of the electronic communications…."). The government obtained subscriber information for each IP address he communicated with. *See* PRTT App. at 5. Even if Gottesfeld had no reasonable expectation of privacy in each individual IP address he visited, collection of this information *in the aggregate* is constitutionally cognizable under *Jones* and *Katz*.

Violation of the Stored Communications Act ("SCA") (Resp. to Govt. Opp. at 19)

The government, in an attempt to free itself from the "specific and articulable facts" standard set forth in the SCA, accuses Gottesfeld of having "conflate[d]" the SCA with the Pen/Trap statute. *See* Govt Opp. at 19. Yet the government sought and obtained information under the SCA. *See* PRTT App. at 5 (seeking an order, "pursuant to 18 U.S.C. §§ 2702(c) and (d), directing that RCN… provide to FBI agents…. [subscriber information]"). The SCA, 18 U.S.C. §2703(d), permits the collection of the subscriber information "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." The government failed to make this showing.

Violation of the Wiretap Act (Resp. to Govt. Opp. at 19 n.5)

Gottesfeld's argument that the surveillance violated the Wiretap Act is the flip-side of his argument that the information the government surveilled was *content*. *See* Mot. at 14-15. If the information collected was indeed content, the government needed a wiretap warrant.

No Probable Cause Absent the PRTT Information (Resp. to Govt. Opp. at 19-21)

The government argues that it had probable cause to search the home based on the Youtube video alone. *See* Govt. Opp. at 20. The defendant disagrees for the reasons set forth in his Motion, and also notes that this argument further supports the notion that the government was simply

fishing for information when it surveilled Gottesfeld. The Youtube video was posted on March 23, 2014. Search Warrant Affidavit ("SW Aff.") ¶ 10. The DDoS attack against Children's Hospital took place on April 24, 2014. *Id.* ¶ 6. The government obtained the Pen/Trap order three months later, on July 17. It knew about the Youtube video at that time but obviously felt the need to try to gather additional evidence before charging Gottesfeld with any crime. Indeed, in applying for the Pen/Trap order, the government could only say that it suspected that the "attack against BCH is suspected to be related to the recent activist effort concerning the custody battle over Justina Pelletier, who was a BCH patient." *See* PRTT App. at 4. If the government had probable cause, notwithstanding the information obtained from the Pen/Trap order, then it would not have had to wait to get the information obtained from their surveillance of Gottesfeld's internet activity to apply for a federal search warrant and pursue criminal charges.

Overbreadth of Search Warrant (Resp. to Govt. Opp. at 21-23)

The government attempts to distinguish this warrant from the one found unconstitutionally overbroad in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017). *See* Govt. Opp. at 22-23; Mot. at 17. It focuses on the holding in *Griffith* that the warrant lacked probable cause because there was no connection alleged between the type of crime at issue and the cell phones/electronic devices. *See* Govt. Opp. at 22-23. Yet the government ignores the alternative holding in *Griffith*: the warrant was "also invalid for [the] additional reason" that it was overbroad in allowing the seizure of all electronic devices found in the residence, regardless of ownership. *Griffith*, 867 F.3d at 1275. The government attempts to defend the same overbreadth in the warrant here by asserting that it should not have to particularize *whose* devices it wants to seize because "'Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant.'" Govt. Opp. at 22 (quoting SW Aff. ¶ 35). The government had no

particular reason to believe that any equipment was "mislabeled" or "used without the owner's knowledge," and indeed this assertion is broad enough to permit the government to seize any number of objects, in *any* search, that do not belong to the subject of the search but may have merely been "mislabeled" or used without the owner's knowledge. "[C]onstrain[ed]" or not, the government must comply with the Constitution.

In sum, Gottesfeld urges the Court to suppress all evidence obtained and derived from the search of Gottesfeld's home.

MARTIN GOTTESFELD,
By His Attorneys,

/s/ Jane F. Peachy
Jane F. Peachy, BBO#661394

/s/ Amy Barsky
Cal. Bar 270846

Federal Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Jane F. Peachy, Esquire, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on October 20, 2017.

/s/ Jane F. Peachy
Jane F. Peachy